



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003
21254	7590	05/10/2005		
MCGINN & GIBB, PLLC 8321 OLD COURTHOUSE ROAD SUITE 200 VIENNA, VA 22182-3817			EXAMINER LAFORGIA, CHRISTIAN A	
			ART UNIT 2131	PAPER NUMBER

DATE MAILED: 05/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/457,732

Applicant(s)

ANDREA CALIFANO

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) 2-4 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 5-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment of 15 April 2005 has been noted and made of record.
2. Claims 1-36 have been presented for examination.
3. Claims 2-4 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments filed 15 April 2005 have been fully considered but they are not persuasive.

5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features, such as how the comparison between the two data sets are compared, upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. In response to the Applicant's assertion that Borza does not disclose whether $h(P)$ is close to $h(P')$ by comparison. First, Borza discloses in column 8, lines 28-30 that in an alternative embodiment, the encrypted characterized biometric information is compared against an encrypted template, thereby teaching the Applicant's limitation of comparing $h(P')$ to $h(P)$. Borza goes on later in column 16, lines 31-38 that: "Identification of an individual is performed by evaluating values from the registration to determine a probability... of false acceptance and false rejection. When the value is within predetermined limits for an acceptable value, identification is provided. Thus Borza discloses determining whether $h(P)$ is close to $h(P')$ by comparison.

Art Unit: 2131

7. In response to the Applicant's allegation that Borza does not disclose or suggest with sufficient specificity how such a comparison could be implemented or accomplished, the Examiner calls upon MPEP § 2121. When the reference relied on expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable. Once such a reference is found, the burden is on applicant to provide facts rebutting the presumption of operability. See *In re Sasse*, 629 F.2d 675, 207 USPQ 107 (CCPA, 1980). See also MPEP § 716.07. See MPEP § 715.07 for examples of the facts needed to prove the inoperability of a reference.

8. See further rejections that follow.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1, 14-16, 31, and 32 are rejected under 35 U.S.C. 101 because the claimed invention is not supported by either a specific and substantial asserted utility or a well established utility.

11. Claims 1, 14-16, 31, and 32 are also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a specific and substantial asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

12. Claims 1 and 5-36 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Acquiring P' and computing h(P') are critical or essential to the

Art Unit: 2131

practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). In accordance with Figure 2, specifically blocks 201 and 202, in order to compare $h(P)$ and $h(P')$, P' must be acquired from the subject and $h(P')$ must be computed in order for a comparison to be made. How can two objects be compared when only one sample (i.e. a control sample) is obtained???

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. The term "substantially" in claims 1, 14-16 is a relative term which renders the claim indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. See MPEP § 2173.05(b), see *Andrew Corp. v. Gabriel Electronics*, 847 F.2d 819, 6 USPQ2d 2010 (Fed. Cir. 1988), *In re Nehrenberg*, 280 F.2d 161, 126 USPQ 383 (CCPA 1960), *In re Mattison*, 509 F.2d 563, 184 USPQ 484 (CCPA 1975).

15. Claims 1, 5-36 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. This is supported by Figure 2, blocks 201, 202, and optionally 203. See MPEP § 2172.01. The omitted steps are:

obtaining a sample of P' such that a comparison can be made;
computing $h(P')$.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Art Unit: 2131

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

16. Claims 1, 14-16, 31, and 32 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claims 1, 14-16, 31, and 32 all generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication. The Examiner holds that such a method could not work, as evident by the **Handbook of Applied Cryptography** to Menezes et al., hereinafter Menezes. Chapter 9 of Menezes discloses the properties of hash functions. On page 331, Menezes proceeds to state one of the properties of one-way hash functions being near-collision resistance. Near-collision resistance is the property that states that “it should be hard to find any two inputs x , x' such that $h(x)$ and $h(x')$ differ in only a small number of bits.” This is further supported by section 9.2.2 **Basic properties and definitions**, on page 323 and 324.

Claim Rejections

17. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

18. Claims 1 and 5-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,446,210 to Borza, hereinafter Borza, in view of U.S. Patent No. 6,487,662 to Kharon et al., hereinafter Kharon.

19. As per claims 1, 13, 14, 16, 18, 20, 24-26, 28, 30-32, 34, and 36, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

Art Unit: 2131

selecting a function h , and for at least one of each said data set P to be collected, computing $h(P)$ (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing $h(P)$ in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

to determine whether P' is close to a predetermined subject, comparing $h(P)$ to all available $h(P)$ s to determine whether P' substantially matches, but does not exactly match, one of said data set P (Figures 12, 13, 16, 17; column 8, lines 28-38, column 14, lines 21-59, column 16, lines 61-37, column 16, lines 53-58, i.e. "when the value is within predetermined limits for an acceptable value, identification is provided....when the value falls outside the predetermined limits identification is not provided");

wherein said data set P cannot be extracted from $h(P)$ (column 8, lines 28-38);

wherein said semiotic data comprises biometric data (column 11, line 65 to column 12, line 18);

wherein said function h comprises a secure hash function (Figure 5; column 7, line 45 to column 8, line 3);

wherein the data set P is not determined perfectly by its reading (column 8, lines 28-38, column 14, lines 21-59, column 16, lines 61-37, column 16, lines 53-58)

wherein each reading gives a number P_i , wherein i is no less than 0, wherein P_0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 8, lines 28-48; column 11, lines 25-34; column 12, lines 25-61),

wherein reading P_0 is different from P_i for $i > 0$, and the secret version of P_0 is different from the secret version of P_i , such that no identification is possibly by a direct comparison of the

Art Unit: 2131

encrypted data (Figures 7b, 9-11, 14, 18; column 13, lines 1-21, column 14, line 60 to column 15, line 63, column 16, line 58 to column 17, line 14),

each time a P_i , with $i > 0$, is read, computing all possible predetermined size variations of P_i which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61),

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user (column 4, lines 46-58; column 5, lines 42-55),

wherein at least one of said data set P and P' comprises a personal data set (column 12, lines 25-34).

20. Borza does not teach extracting sub-collections S_j from the collection of data in data set P ; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

21. Kharon teaches further comprising:

extracting sub-collections S_j from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67);

Art Unit: 2131

comparing encrypted versions of the sub-collections S_j with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection S_j matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

22. As per claim 5, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h , and for at least one of each said data set P to be collected, computing $h(P)$ (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing $h(P)$ in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from $h(P)$ (column 8, lines 28-38);

the method further comprising:

selecting a private key/public key (K, k) once for all cases (column 4, lines 26-32); and

choosing said function h as the public encryption function corresponding to k (column 5, lines 28-54).

23. Borza does not teach destroying said private key K and sending said private key K to a trusted party. It would have been obvious to one having ordinary skill in the art at the time the invention was made to destroy the private key K and send it the private key K to a trusted third party, since it is known in the art that the private key is needed to decrypt any message encrypted with public key k, therefore the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k.

24. Regarding claim 6, Borza teaches wherein said data set P cannot be extracted from $h(P)$, except by the trusted party (column 8, lines 28-38).

25. Regarding claim 7, Borza teaches to determine whether some P' is a predetermined subject, comparing said $h(P)$ to all available $h(P)$ s (column 12, lines 48-61); and determining whether there is a match (column 12, lines 48-61).

26. Regarding claim 8, Borza does not teach wherein the trusted party comprises a panel of members, and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the trusted party to comprise of a panel of members, and share a secret is amongst the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret, since it has been held that mere duplication of essential elements (e.g. trusted third party)

Art Unit: 2131

involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. See also MPEP § 2144.04.

27. As per claim 9, Borza teaches a method of processing semiotic data, comprising:

- receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);
- selecting a function h, and for at least one of each said data set P to be collected,
- computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);
- destroying said data set P (column 2, lines 27-29); and
- storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and
- wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);
- wherein the data set P is not determined perfectly by its reading (column 11, lines 25-34),
- wherein each reading gives a number P_i , wherein i is no less than 0, wherein P_0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),
- wherein reading P_0 is different from P_i for $i > 0$, and the secret version of P_0 is different from the secret version of P_i , such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

28. Regarding claim 10, Borza does not teach extracting sub-collections S_j from the collection of data in data set P; and encrypting a predetermined number of such sub-collections

Art Unit: 2131

such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

29. Kharon teaches extracting sub-collections S_j from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

30. With regards to claims 11 and 21, Borza does not teach comparing encrypted versions of the sub-collections S_j with those data stored in said database, wherein if one or more of the sub-collection S_j matches with said data, then verification is deemed to have occurred.

31. Kharon teaches comparing encrypted versions of the sub-collections S_j with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection S_j matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

32. Concerning claims 12 and 23, Borza teaches each time a P_i , with $i > 0$, is read, computing all possible predetermined size variations of P_i which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61).

33. As per claims 15, 17, 27, and 33, Borza teaches a method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29);

storing each of the at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38),

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match (Figure 12; column 8, lines 28-38).

Art Unit: 2131

34. As per claims 19, 29, and 35, Borza teaches a method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29); and

storing each said at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38).

35. Borza does not teach extracting sub-collections S_j from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

36. Kharon teaches further comprising:

extracting sub-collections S_j from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be

Art Unit: 2131

motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

37. Regarding claim 22, Borza teaches wherein the data set P is not determined perfectly by its reading, such that each reading gives a number P_i ,

wherein i is no less than 0 (column 11, line 65 to column 12, line 34),

wherein P_0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading P_0 is different from P_i for $i > 0$, and the secret version of P_0 is different from the secret version of P_i , such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

Conclusion

38. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

39. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Art Unit: 2131


40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

41. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

42. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100